

Linear time Constructions of some d -Restriction Problems

Nader H. Bshouty
Dept. of Computer Science
Technion, Haifa, 32000

June 12, 2014

Abstract

We give new linear time globally explicit constructions of some d -restriction problems that follows from the techniques used in [1, 30, 31].

Keywords: Derandomization, d -Restriction problems, Perfect hash, Cover-Free families, Separating hash functions.

1 Introduction

A d -restriction problem [30, 2, 6] is a problem of the following form:

Given an alphabet Σ of size $|\Sigma| = q$, an integer n and a class \mathcal{M} of nonzero functions $f : \Sigma^d \rightarrow \{0, 1\}$.

Find a small set $A \subseteq \Sigma^n$ such that: For every $1 \leq i_1 < i_2 < \dots < i_d \leq n$ and $f \in \mathcal{M}$ there is $a \in A$ such that $f(a_{i_1}, \dots, a_{i_d}) \neq 0$.

A $(1 - \epsilon)$ -dense d -restriction problem is a problem of the following form:

Given an alphabet Σ of size $|\Sigma| = q$, an integer n and a class \mathcal{M} of nonzero functions $f : \Sigma^d \rightarrow \{0, 1\}$.

Find a small set $A \subseteq \Sigma^n$ such that: For every $1 \leq i_1 < i_2 < \dots < i_d \leq n$ and $f \in \mathcal{M}$

$$\Pr_{a \in A}[f(a_{i_1}, \dots, a_{i_d}) \neq 0] > 1 - \epsilon$$

where the probability is over the choice of a from the uniform distribution on A .

We give new constructions for the following three $((1 - \epsilon)$ -dense) d -restriction problems: Perfect hash family, cover-free family and separating hash family.

A construction is *global explicit* if it runs in deterministic polynomial time in the size of the construction. A *local explicit construction* is a construction where one can find any bit in the construction in time poly-log in the size of the construction. The constructions in this paper are linear time global explicit constructions.

To the best of our knowledge, our constructions have sizes that are less than the ones known from the literature.

2 Old and New Results

2.1 Perfect Hash Family

Let H be a family of functions $h : [n] \rightarrow [q]$. For $d \leq q$ we say that H is an (n, q, d) -*perfect hash family* ((n, q, d) -PHF) [2] if for every subset $S \subseteq [n]$ of size $|S| = d$ there is a *hash function* $h \in H$ such that $h|_S$ is injective (one-to-one) on S , i.e., $|h(S)| = d$.

Blackburn and Wild [12] gave an optimal explicit construction when

$$q \geq 2^{O(\sqrt{d \log d \log n})}.$$

Stinson et al., [32], gave an explicit construction of (n, q, d) -PHF of size $d^{\log^* n} \log n$ for $q \geq d^2 \log n / \log q$. It follows from the technique used in [1] with Reed-Solomon codes that an explicit (n, q, d) -PHF of size $d^2 \log n / \log q$ exist for $q \geq d^2 \log n / \log q$. In [4, 30, 2] it was shown that there are $(n, \Omega(d^2), d)$ -PHF of size $O(d^6 \log n)$ that can be constructed in $\text{poly}(n)$ time. Wang and Xing [36] used algebraic function fields and gave an (n, d^4, d) -PHF of size $O((d^2 / \log d) \log n)$ for infinite sequence of integers n . Their construction is not linear time construction. The above constructions are either for large q or are not linear time constructions.

Bshouty in [6] shows that for a constant $c > 1$, the following (third column in the table) (n, q, d) -PHF can be locally explicitly constructed in almost linear time (within $\text{poly}(\log)$)

n	q	Linear time. Size = $O()$	Upper Bound	Lower Bound
I.S.	$q \geq \frac{c}{4}d^4$	$d^2 \frac{\log n}{\log q}$	$d \frac{\log n}{\log q}$	$d \frac{\log n}{\log q}$
all	$q \geq \frac{c}{4}d^4$	$d^4 \frac{\log n}{\log q}$	$d \frac{\log n}{\log q}$	$d \frac{\log n}{\log q}$
I.S.	$q \geq \frac{c}{2}d^2$	$d^4 \frac{\log n}{\log d}$	$d \frac{\log n}{\log(2q/(d(d-1)))}$	$d \frac{\log n}{\log q}$
all	$q \geq \frac{c}{2}d^2$	$d^6 \frac{\log n}{\log d}$	$d \frac{\log n}{\log(2q/(d(d-1)))}$	$d \frac{\log n}{\log q}$
I.S.	$q = \frac{d(d-1)}{2} + 1 + o(d^2)$	$d^6 \frac{\log n}{\log d}$	$d \log n$	$d \frac{\log n}{\log q}$
all	$q = \frac{d(d-1)}{2} + 1 + o(d^2)$	$d^8 \frac{\log n}{\log d}$	$d \log n$	$d \frac{\log n}{\log q}$

The upper bound in the table follows from union bound [6]. The lower bound is from [25, 5] (see also [27, 17, 20, 21, 12, 11, 7]). I.S. stands for “true for infinite sequence of integers n ”.

Here we prove

Theorem 1. *Let q be a power of prime. If $q > 4(d(d-1)/2 + 1)$ then there is a (n, q, d) -PHF of size*

$$O\left(\frac{d^2 \log n}{\log(q/e(d(d-1)/2 + 1))}\right)$$

that can be constructed in linear time.

If $d(d-1)/2 + 2 \leq q \leq 4(d(d-1)/2 + 1)$ then there is a (n, q, d) -PHF of size

$$O\left(\frac{q^2 d^2 \log n}{(q - d(d-1)/2 - 1)^2}\right)$$

that can be constructed in linear time.

In particular, for any constants $c > 1$, $\delta > 0$ and $0 \leq \eta < 1$, the following (n, q, d) -PHF can be constructed in linear time (the third column in the following table)

n	q	Linear time. Size = $O()$	Upper Bound	Lower Bound
all	$q \geq d^{2+\delta}$	$d^2 \frac{\log n}{\log q}$	$d \frac{\log n}{\log q}$	$d \frac{\log n}{\log q}$
all	$q \geq \frac{c}{2}d^2$	$d^2 \log n$	$d \log n$	$d \frac{\log n}{\log q}$
all	$q = \frac{d(d-1)}{2} + 1 + d^{2\eta}$	$d^{6-4\eta} \log n$	$d \log n$	$d \frac{\log n}{\log q}$
all	$q = \frac{d(d-1)}{2} + 2$	$d^6 \frac{\log n}{\log d}$	$d \log n$	$d \frac{\log n}{\log q}$

Notice that for $q > cd^2/2$, $c > 1$ the sizes in the above theorem is within a factor of d of the lower bound. Constructing almost optimal (within $\text{poly}(d)$)

(n, q, d) -PHF for $q = o(d^2)$ is still a challenging open problem. Some nearly optimal constructions of (n, q, d) -PHF for $q = o(d^2)$ are given in [30, 24].

The (n, q, d) -perfect hash families for $d \leq 6$ are studied in [3, 12, 5, 32, 24, 10, 9, 26]. In this paper we prove

Theorem 2. *If q is prime power and $d \leq \log n / (8 \log \log n)$ then there is a linear time construction of (n, q, d) -PHF of size*

$$O\left(\frac{d^3 \log n}{g(q, d)}\right)$$

where

$$g(q, d) = \left(1 - \frac{1}{q}\right) \left(1 - \frac{2}{q}\right) \cdots \left(1 - \frac{d-1}{q}\right).$$

Using the lower bound in [17] we show that the size in the above theorem is within a factor of d^4 of the lower bound when $q = d + O(1)$ and within a factor of d^3 for $q > cd$ for some $c > 1$.

2.2 Dense Perfect Hash Family

We say that H is an $(1 - \epsilon)$ -dense (n, q, d) -PHF if for every subset $S \subseteq [n]$ of size $|S| = d$ there are at least $(1 - \epsilon)|H|$ hash functions $h \in H$ such that $h|_S$ is injective on S .

We prove

Theorem 3. *Let q be a power of prime. If $\epsilon > 4(d(d-1)/2 + 1)/q$ then there is a $(1 - \epsilon)$ -dense (n, q, d) -PHF of size*

$$O\left(\frac{d^2 \log n}{\epsilon \log(\epsilon q / e(d(d-1)/2 + 1))}\right)$$

that can be constructed in linear time.

If $(d(d-1)/2 + 1)/(q-1) \leq \epsilon \leq 4(d(d-1)/2 + 1)/q$ then there is a $(1 - \epsilon)$ -dense (n, q, d) -PHF of size

$$O\left(\frac{q^2 d^2 \log n}{\epsilon(q - (d(d-1)/2 + 1)/\epsilon)^2}\right)$$

that can be constructed in linear time.

We also prove (what we believe) two folklore results that show that the bounds on the size and ϵ in the above theorem are almost tight. First, we show that the size of any $(1 - \epsilon)$ -dense (n, q, d) -PHF is

$$\Omega\left(\frac{d \log n}{\epsilon \log q}\right).$$

Second, we show that no $(1 - \epsilon)$ -dense (n, q, d) -PHF exists when $\epsilon < d(d - 1)/(2q) + O((d^2/q)^2)$.

Notice that for $q \geq (d/\epsilon)^{1+c}$, where $c > 1$ is any constant, the size of the construction in Theorem 3,

$$O\left(\frac{d^2 \log n}{\epsilon \log q}\right),$$

is within a factor d of the lower bound. Also the bound on ϵ is asymptotically tight.

For the rest of this section we will only state the results for the non-dense d -restriction problems. Results similar to Theorem 3 can be easily obtained using the same technique.

2.3 Cover-Free Families

Let X be a set with N elements and let \mathcal{B} be a set of subsets (blocks) of X . We say that (X, \mathcal{B}) is (w, r) -cover-free family $((w, r)$ -CFF), [22], if for any w blocks $B_1, \dots, B_w \in \mathcal{B}$ and any other r blocks $A_1, \dots, A_r \in \mathcal{B}$, we have

$$\bigcap_{i=1}^w B_i \not\subseteq \bigcup_{j=1}^r A_j.$$

Let $N((w, r), n)$ denotes the minimum number of points in any (w, r) -CFF having n blocks. Here we will study CFF when $w = o(r)$ (or $r = o(w)$). We will write $(n, (w, r))$ -CFF when we want to emphasize the number of blocks.

When $w = 1$, the problem is called *group testing*. The problem of group testing which was first presented during World War II was presented as follows [13, 28]: Among n soldiers, at most r carry a fatal virus. We would like to blood test the soldiers to detect the infected ones. Testing each one separately will give n tests. To minimize the number of tests we can mix the blood of several soldiers and test the mixture. If the test comes negative then none of the tested soldiers are infected. If the test comes out positive, we know that at least one of them is infected. The problem is to come up with a small number of tests.

This problem is equivalent to $(n, (1, r))$ -CFF and is equivalent to finding a small set $\mathcal{F} \subseteq \{0, 1\}^n$ such that for every $1 \leq i_1 < i_2 < \dots < i_d \leq n$, $d = r + 1$, and every $1 \leq j \leq d$ there is $a \in \mathcal{F}$ such that $a_{i_k} = 0$ for all $k \neq j$ and $a_{i_j} = 1$.

Group testing has the following lower bound [14, 15, 16]

$$N((1, r), n) \geq \Omega\left(\frac{r^2}{\log r} \log n\right). \quad (1)$$

It is known that a group testing of size $O(r^2 \log n)$ can be constructed in linear time [13, 31, 19].

An $(n, (w, r))$ -CFF can be regarded as a set $\mathcal{F} \subseteq \{0, 1\}^n$ such that for every $1 \leq i_1 < i_2 < \dots < i_d \leq n$ where $d = w + r$ and every $J \subset [d]$ of size $|J| = w$ there is $a \in \mathcal{F}$ such that $a_{i_k} = 0$ for all $k \notin J$ and $a_{i_j} = 1$ for all $j \in J$. Then $N((w, r), n)$ is the minimum size of such \mathcal{F} .

It is known that, [34],

$$N((w, r), n) \geq \Omega \left(\frac{d \binom{d}{w}}{\log \binom{d}{w}} \log n \right).$$

Using union bound it is easy to show

Lemma 1. *For $d = w + r = o(n)$ we have*

$$N((w, r), n) \leq O \left(\sqrt{wrd} \cdot \binom{d}{w} \log n \right).$$

It follows from [32], that for infinite sequence of integers n , an $(n, (w, r))$ -CFF of size

$$M = O \left((wr)^{\log^* n} \log n \right)$$

can be constructed in polynomial time. For constant d , the (n, d) -universal set over $\Sigma = \{0, 1\}$ constructed in [29] of size $M = O(2^{3d} \log n)$ (and in [30] of size $M = 2^{d+O(\log^2 d)} \log n$) is $(n, (w, r))$ -CFF for any w and r of size $O(\log n)$. See also [23]. In [6], Bshouty gave the following locally explicit constructions of $(n, (w, r))$ -CFF that can be constructed in (almost) linear time in their sizes (the third column in the table).

n	w	Linear time Size=	Upper Bound	Lower Bound
I.S	$O(1)$	$\frac{r^{w+2}}{\log r} \log n$	$r^{w+1} \log n$	$\frac{r^{w+1}}{\log r} \log n$
all	$O(1)$	$\frac{r^{w+3}}{\log r} \log n$	$r^{w+1} \log n$	$\frac{r^{w+1}}{\log r} \log n$
I.S.	$o(r)$	$\frac{w^2 (ce)^w r^{w+2}}{\log r} \log n$	$\frac{r^{w+1}}{(w/e)^{w-1/2}} \log n$	$\frac{r^{w+1}}{(w/e)^{w+1} \log r} \log n$
all	$o(r)$	$\frac{w^3 (ce)^w r^{w+3}}{\log r} \log n$	$\frac{r^{w+1}}{(w/e)^{w-1/2}} \log n$	$\frac{r^{w+1}}{(w/e)^{w+1} \log r} \log n$

In the table, $c > 1$ is any constant. We also added to the table the non-constructive upper bound in the forth column and the lower bound in the fifth column.

In this paper we prove

Theorem 4. For any constant $c > 1$, the following $(n, (w, r))$ -CFF can be constructed in linear time in their sizes

n	w	Linear time. Size= $O(\)$	Upper Bound	Lower Bound
<i>all</i>	$O(1)$	$r^{w+1} \log n$	$r^{w+1} \log n$	$\frac{r^{w+1}}{\log r} \log n$
<i>all</i>	$o(r)$	$(ce)^w r^{w+1} \log n$	$\frac{r^{w+1}}{(w/e)^{w-1/2}} \log n$	$\frac{r^{w+1}}{(w/e)^{w+1} \log r} \log n$

Notice that when $w = O(1)$ the size of the construction matches the upper bound obtained with union bound and is within a factor of $\log r$ of the lower bound.

2.4 Separating Hash Family

Let X and Σ be sets of cardinalities n and q , respectively. We call a set \mathcal{F} of functions $f : X \rightarrow \Sigma$ an $(M; n, q, (d_1, d_2, \dots, d_r))$ -separating hash family (SHF), [35, 33], if $|\mathcal{F}| = M$ and for all pairwise disjoint subsets $C_1, C_2, \dots, C_r \subseteq X$ with $|C_i| = d_i$ for $i = 1, 2, \dots, r$, there is at least one function $f \in \mathcal{F}$ such that $f(C_1), f(C_2), \dots, f(C_r)$ are pairwise disjoint subsets. The goal is to find $(M; n, q, (d_1, d_2, \dots, d_r))$ -SHF with small M . The minimal M is denoted by $M(n, q, (d_1, d_2, \dots, d_r))$.

Notice that (n, q, d) -PHF of size M is $(M; n, q, (1, 1, \dots, 1))$ -SHF and (w, r) -CFF of size M is $(M; n, 2, (r, w))$ -SHF.

In [11], Bazrafshan and Trund proved that for

$$\begin{aligned}
 D_1 &= \sum_{i=1}^r d_i, \\
 M(n, q, (d_1, d_2, \dots, d_r)) &\geq (D_1 - 1) \frac{\log n - \log(D_1 - 1) - \log q}{\log q} \\
 &= \Omega\left(D_1 \frac{\log n}{\log q}\right). \tag{2}
 \end{aligned}$$

See also [7].

In [32], Stinson et. al. proved that an $(M; n, q, (d_1, d_2))$ separating hash families of size

$$M = O((d_1 d_2)^{\log^* n} \log n)$$

can be constructed in polynomial time for infinite sequence of integers n and $q > d_1 d_2$. The same proof gives a polynomial time construction for any separating hash family of size

$$M = O(D_2^{\log^* n} \log n)$$

where

$$D_2 = \sum_{1 \leq i_1 < i_2 \leq r} d_{i_1} d_{i_2}$$

when $q > D_2$.

In [23], Liu and Shen provide an explicit constructions of $(M; n, q, (d_1, d_2))$ separating hash families using algebraic curves over finite fields. They show that for infinite sequence of integers n there is an explicit $(M; n, q, (d_1, d_2))$ separating hash families of size $O(\log n)$ for fixed d_1 and d_2 . This also follows from [29], an $(n, d_1 + d_2)$ -universal set over two symbols alphabet is a separating hash families of size $O(\log n)$ for fixed d_1 and d_2 . Their construction is similar to the construction of the tester in [6]. In [6] Bshouty gave a polynomial time construction of an $(M; n, q, (d_1, d_2))$ separating hash families of size $M = ((d_1 d_2)^4 \log n / \log q)$ for any $q \geq d_1 d_2 (1 + o(1))$ and any n . He also show that for any constant $c > 1$ and $q > D_2$, the following $(M; n, q, (d_1, d_2, \dots, d_r))$ separating hash family can be constructed in polynomial time

n	q	poly time. Size $M = O()$	Upper Bound	Lower Bound
I.S.	$q \geq c(D_2 + 1)^2, q \text{ P.S.}$	$D_2 \frac{\log n}{\log q}$	$D_1 \frac{\log n}{\log q}$	$D_1 \frac{\log n}{\log q}$
all	$q \geq c(D_2 + 1)^2, q \text{ P.S.}$	$D_2^2 \frac{\log n}{\log q}$	$D_1 \frac{\log n}{\log q}$	$D_1 \frac{\log n}{\log q}$
I.S.	$q \geq c(D_2 + 1)$	$D_2^2 \frac{\log n}{\log D_2}$	$D_1 \log n$	$D_1 \frac{\log n}{\log q}$
all	$q \geq c(D_2 + 1)$	$D_2^3 \frac{\log n}{\log D_2}$	$D_1 \log n$	$D_1 \frac{\log n}{\log q}$
I.S.	$q \geq D_2 + 1$	$D_2^3 \frac{\log n}{\log D_2}$	$D_1 \log n$	$D_1 \frac{\log n}{\log q}$
all	$q \geq D_2 + 1$	$D_2^4 \frac{\log n}{\log D_2}$	$D_1 \log n$	$D_1 \frac{\log n}{\log q}$

and an $(M; n, r, (d_1, d_2, \dots, d_r))$ separating hash family of size

$$M = \frac{\binom{cD_2}{d_1 \ d_2 \ \dots \ d_r} D_2^3}{\log D_2} \log n,$$

can be constructed in time linear in the construction size.

Here we prove the following

Theorem 5. *For any constant $c > 1$ and $q > D_2$, the following $(M; n, q, (d_1, d_2, \dots, d_r))$ separating hash family can be constructed in linear time*

n	q	poly time. Size $M = O()$	Upper Bound	Lower Bound
<i>all</i>	$q \geq (D_2 + 1)^c$	$D_2 \frac{\log n}{\log q}$	$D_1 \frac{\log n}{\log q}$	$D_1 \frac{\log n}{\log q}$
<i>all</i>	$q \geq c(D_2 + 1)$	$D_2 \log n$	$D_1 \log n$	$D_1 \frac{\log n}{\log q}$
<i>all</i>	$q \geq D_2 + 2$	$D_2^3 \log n$	$D_1 \log n$	$D_1 \frac{\log n}{\log q}$

and an $(M; n, r, (d_1, d_2, \dots, d_r))$ separating hash family of size

$$M = \begin{pmatrix} cD_2 \\ d_1 & d_2 & \dots & d_r \end{pmatrix} D_2 \log n,$$

can be constructed in time linear in the construction size.

3 Preliminary Constructions

A linear code over the field \mathbb{F}_q is a linear subspace $C \subset \mathbb{F}_q^m$. Elements in the code are called *words*. A linear code C is called $[m, k, d]_q$ linear code if $C \subset \mathbb{F}_q^m$ is a linear code, $|C| = q^k$ and for every two words v and u in the code $\text{dist}(v, u) := |\{i \mid v_i \neq u_i\}| \geq d$.

The q -ary entropy function is

$$H_q(p) = p \log_q \frac{q-1}{p} + (1-p) \log_q \frac{1}{1-p}.$$

The following is from [31] (Theorem 2)

Lemma 2. *Let q be a prime power, m and k positive integers and $0 \leq \delta \leq 1$. If $k \leq (1 - H_q(\delta))m$, then an $[m, k, \delta m]_q$ linear code can be globally explicit constructed in time $O(mq^k)$.*

Notice that to construct n codewords in an $[m, k, \delta m]_q$ linear code where $q^{k-1} < n \leq q^k$, the time of the construction is $O(mq^k) = O(qmn)$.

We now show

Lemma 3. *Let q be a prime power, m and k positive integers, $0 \leq \delta \leq 1$ and n an integer such that $q^{k-1} < n \leq q^k$. If $k \leq (1 - H_q(\delta))m$, then a set of n codewords in an $[m, k, \delta m]_q$ linear code can be globally explicit constructed in time $O(mn)$.*

Proof. The same proof of Lemma 3 in [31] works here with the observation that the first column of the generator matrix $G = [v_1 \mid \dots \mid v_k]$ can be the all-one vector $v_1 = (1, 1, \dots, 1)'$ and it is enough to ensure that every codeword of the form $\sum_{i=1}^k \lambda_i v_i$, where the first nonzero λ_i is 1, is of weight at least δm . We call such codeword a normalized codeword. The number of normalized codewords is $(q^k - 1)/(q - 1) = O(q^{k-1})$. Obviously, codeword v is equal to λu for some normalized codewords u and the minimum weight of normalized codeword is the minimum weight of the code.

Therefore we first construct the normalized codewords as in [31] in time $O(mq^{k-1})$ and then add any $n - (q^k - 1)/(q - 1)$ codewords. \square

All the results in this paper uses Lemma 3 and therefore they are globally explicit constructions. We now show

Lemma 4. *Let q be a prime power, $1 < h < q/4$ and*

$$m = \left\lceil \frac{h \ln(q(n+1))}{\ln q - \ln h - 1} \right\rceil.$$

A set of n nonzero codewords of a

$$\left[m, \left\lceil \frac{\log(n+1)}{\log q} \right\rceil, \left(1 - \frac{1}{h}\right) m \right]_q$$

linear code can be constructed in time $O(nm)$.

Proof. By Lemma 3 it is enough to show that

$$\left\lceil \frac{\log(n+1)}{\log q} \right\rceil \leq \left(1 - H_q\left(1 - \frac{1}{h}\right)\right) m.$$

Now since for $x > 0$, $(x-1)/x \leq \ln x$ we have

$$\begin{aligned} 1 - H_q\left(1 - \frac{1}{h}\right) &= 1 - \left(\left(1 - \frac{1}{h}\right) \log_q \frac{q-1}{1-1/h} + \frac{1}{h} \log_q h \right) \\ &= \frac{1}{h} - \frac{1}{h} \log_q h - \left(1 - \frac{1}{h}\right) \log_q \frac{1-1/q}{1-1/h} \\ &\geq \frac{1}{h} - \frac{1}{h} \log_q h + \frac{h-1}{h} \log_q (1-1/h) \\ &\geq \frac{1}{h} - \frac{1}{h} \log_q h - \frac{1}{h \ln q} \\ &= \frac{\ln q - \ln h - 1}{h \ln q}. \end{aligned}$$

Now

$$\left(1 - H_q\left(1 - \frac{1}{h}\right)\right) m \geq \frac{\ln q(n+1)}{\ln q} \geq \left\lceil \frac{\log(n+1)}{\log q} \right\rceil.$$

□

When $h = O(q)$ we show

Lemma 5. *Let q be a prime power, $2 \leq q/4 \leq h \leq q-1$ and*

$$m = \left\lceil \frac{4(q-1)^2 h \ln(q(n+1))}{(q-h)^2} \right\rceil.$$

A set of n nonzero codewords of a

$$\left[m, \left\lceil \frac{\log(n+1)}{\log q} \right\rceil, \left(1 - \frac{1}{h}\right) m \right]_q$$

linear code can be constructed in time $O(nm)$.

Proof. For $\Delta = 1 - H_q\left(1 - \frac{1}{h}\right)$ and using the fact that $\ln(1-x) = -x - x^2/2 - x^3/3 - \dots$ for $|x| < 1$, we have

$$\begin{aligned} \Delta &= \frac{1}{h} - \frac{1}{h} \log_q h - \left(1 - \frac{1}{h}\right) \log_q \frac{1 - 1/q}{1 - 1/h} \\ &= \frac{1}{\ln q} \left(\frac{1}{h} \ln \frac{q}{h} - \left(1 - \frac{1}{h}\right) \ln \frac{h(q-1)}{q(h-1)} \right) \\ &= \frac{1}{\ln q} \left(-\frac{1}{h} \ln \left(1 - \frac{q-h}{q-1}\right) + \ln \left(1 - \frac{q-h}{h(q-1)}\right) \right) \\ &= \frac{(q-h)^2}{(q-1)^2 h \ln q} \left(\frac{1}{2} \left(1 - \frac{1}{h}\right) + \frac{q-h}{3(q-1)} \left(1 - \frac{1}{h^2}\right) + \dots \right) \\ &\geq \frac{(q-h)^2}{(q-1)^2 h \ln q} \left(\frac{1}{2} \left(1 - \frac{1}{h}\right) \right) \geq \frac{(q-h)^2}{4(q-1)^2 h \ln q}. \end{aligned}$$

Now

$$\left(1 - H_q\left(1 - \frac{1}{h}\right)\right) m \geq \frac{\ln q(n+1)}{\ln q} \geq \left\lceil \frac{\log(n+1)}{\log q} \right\rceil.$$

□

4 Main Results

In this section we give two main results that will be used throughout the paper

Let $I \subseteq [n]^2$. Define the following homogeneous polynomial

$$H_I = \prod_{(i_1, i_2) \in I} (x_{i_1} - x_{i_2}).$$

We denote by $\mathcal{H}_d \subseteq \mathbb{F}_q[x_1, \dots, x_n]$ the class of all such polynomials of degree at most d . A *hitting set* for \mathcal{H}_d over \mathbb{F}_q is a set of assignment $A \subseteq \mathbb{F}_q^n$ such that for every $H \in \mathcal{H}_d, H \neq 0$, there is $a \in A$ where $H(a) \neq 0$. A $(1-\epsilon)$ -*dense hitting set* for \mathcal{H}_d over \mathbb{F}_q is a set of assignment $A \subseteq \mathbb{F}_q^n$ such that for every $H \in \mathcal{H}_d, H \neq 0$,

$$\Pr_{a \in A}[H(a) \neq 0] > 1 - \epsilon$$

where the probability is over the choice of a from the uniform distribution on A . When $H(a) \neq 0$ then we say that the assignment a *hits* H and H is *not zero on* a .

We prove

Lemma 6. *Let $n > q, d$. If $q > 4(d+1)$ is prime power then there is a hitting set for \mathcal{H}_d of size*

$$m = \left\lceil \frac{(d+1) \log(q(n+1))}{\log(q/e(d+1))} \right\rceil = O\left(\frac{d \log n}{\log(q/e(d+1))}\right)$$

that can be constructed in time $O(mn) = O(dqn \log(qn))$.

If $d+2 \leq q \leq 4(d+1)$ is prime power then there is a hitting set for \mathcal{H}_d of size

$$m = \left\lceil \frac{4(q-1)^2(d+1) \ln(q(n+1))}{(q-d-1)^2} \right\rceil = O\left(\frac{dq^2 \log n}{(q-d-1)^2}\right)$$

that can be constructed in time $O(mn) = O(d(q^2/(q-d-1)^2)n \log(qn))$.

Proof. Consider the code C

$$\left[m, \left\lceil \frac{\log(n+1)}{\log q} \right\rceil, \left(1 - \frac{1}{d+1}\right) m \right]_q$$

constructed in Lemma 4 and Lemma 5. The number of non-zero words in the code is at least n . Take any n distinct non-zero words $c^{(1)}, \dots, c^{(n)}$ in C and define the assignments $a^{(i)} \in \mathbb{F}_q^n$, $i = 1, \dots, m$ where $a_j^{(i)} = c_i^{(j)}$. Let $H_I \in \mathcal{H}_d$, $H_I \neq 0$. Then

$$H_I = \prod_{(i_1, i_2) \in I} (x_{i_1} - x_{i_2}) \neq 0$$

where $|I| \leq d$. For each $t := x_{i_1} - x_{i_2}$ we have $(t(a^{(1)}), \dots, t(a^{(m)}))^T = c^{(i_1)} - c^{(i_2)} \in C$ is a non-zero word in C and therefore t is zero on at most $m/(d+1)$ assignments. Therefore H_I is zero on at most $dm/(d+1) < m$ assignment. This implies that there is an assignment in A that hits H_I . \square

Notice that the size of the hitting set is mn and therefore the time complexity in the above lemma is linear in the size of the hitting set.

In the same way one can prove

Lemma 7. *Let q be a prime power. If $q > 4(d+1)/\epsilon$ be a prime power. Let $n > q, d$. There is a $(1 - \epsilon)$ -dense hitting set for \mathcal{H}_d of size*

$$m = \left\lceil \frac{(d+1) \log(q(n+1))}{\epsilon \log(\epsilon q/e(d+1))} \right\rceil = O\left(\frac{d \log n}{\epsilon \log(\epsilon q/e(d+1))}\right)$$

that can be constructed in time $O(dqn \log(qn)/\epsilon)$.

If $(d+1)/\epsilon + 1 \leq q \leq 4(d+1)/\epsilon$ be a prime power. Let $n > q, d$. There is a $(1 - \epsilon)$ -dense hitting set for \mathcal{H}_d of size

$$m = \left\lceil \frac{4(q-1)^2(d+1) \ln(q(n+1))}{(q - (d+1)/\epsilon)^2 \epsilon} \right\rceil = O\left(\frac{dq^2 \log n}{(q - (d+1)/\epsilon)^2 \epsilon}\right)$$

that can be constructed in time $O(d(q^2/(q-d-1)^2)n \log(qn)/\epsilon)$.

We note here that such result cannot be achieved when $q < d/\epsilon$ [6].

5 Proof of the Theorems

5.1 Perfect Hash Family

Here we prove

Theorem 1. *Let q be a power of prime. If $q > 4(d(d-1)/2 + 1)$ then there is a (n, q, d) -PHF of size*

$$O\left(\frac{d^2 \log n}{\log(q/e(d(d-1)/2 + 1))}\right)$$

that can be constructed in linear time.

If $d(d-1)/2 + 2 \leq q \leq 4(d(d-1)/2 + 1)$ then there is a (n, q, d) -PHF of size

$$O\left(\frac{q^2 d^2 \log n}{(q - d(d-1)/2 - 1)^2}\right)$$

that can be constructed in linear time.

In particular, for any constants $c > 1$, $\delta > 0$ and $0 \leq \eta < 1$, the following (n, q, d) -PHF can be constructed in linear time (the third column in the following table)

n	q	Linear time. Size = $O()$	Upper Bound	Lower Bound
all	$q \geq d^{2+\delta}$	$d^2 \frac{\log n}{\log q}$	$d \frac{\log n}{\log q}$	$d \frac{\log n}{\log q}$
all	$q \geq \frac{c}{2} d^2$	$d^2 \log n$	$d \log n$	$d \frac{\log n}{\log q}$
all	$q = \frac{d(d-1)}{2} + 1 + d^{2\eta}$	$d^{6-4\eta} \log n$	$d \log n$	$d \frac{\log n}{\log q}$
all	$q = \frac{d(d-1)}{2} + 2$	$d^6 \frac{\log n}{\log d}$	$d \log n$	$d \frac{\log n}{\log q}$

Proof. Consider the set of functions

$$\mathcal{F} = \{\Delta_{\{i_1, \dots, i_d\}}(x_1, \dots, x_n) \mid 1 \leq i_1 < \dots < i_d \leq n\}$$

in $\mathbb{F}_q[x_1, x_2, \dots, x_n]$ where

$$\Delta_{\{i_1, \dots, i_d\}}(x_1, \dots, x_n) = \prod_{1 \leq k < j \leq d} (x_{i_k} - x_{i_j}).$$

It is clear that a hitting set for \mathcal{F} is (n, q, d) -PHF. Now since $\mathcal{F} \subseteq \mathcal{H}_{d(d-1)/2+1}$ the result follows from Lemma 6. \square

When $q > d(d-1)/2$ is not a power of prime number then we can take the nearest prime $q' < q$ and construct an (n, q', d) -PHF that is also (n, q, d) -PHF. It is known that the nearest prime $q' \geq q - \Theta(q^{.525})$, [8], and therefore the result in the above table is also true for any integer $q \geq d(d+1)/2 + O(d^{1.05})$.

5.2 Perfect Hash Family for Small d

We now prove

Theorem 2. *If q is prime power and $d \leq \log n / (8 \log \log n)$ then there is a linear time construction of (n, q, d) -PHF of size*

$$O\left(\frac{d^3 \log n}{g(q, d)}\right)$$

where

$$g(q, d) = \left(1 - \frac{1}{q}\right) \left(1 - \frac{2}{q}\right) \dots \left(1 - \frac{d-1}{q}\right).$$

Proof. If $q > d^2$ then the construction in Theorem 1 has the required size. Let $q \leq d^2$. We first use Theorem 1 to construct an (n, d^3, d) -PHF H_1 of size $O(d^2 \log n / \log d)$ in linear time. Then a (d^3, q, d) -PHF H_2 of size $O(d \log d / g(q, d))$ can be constructed in time, [30, 2],

$$\binom{d^3}{d} q^{1 + \lceil \log d^3 / \log q \rceil (d-1)} \leq d^{3d} q^d d^{3d} \leq d^{8d} < n.$$

Then $H = \{h_2(h_1) \mid h_2 \in H_2, h_1 \in H_1\}$ is (n, q, d) -PHF of the required size. \square

We now show that this bound is within a factor of d^4 of the lower bound when $q = d + O(1)$ and within a factor of $d^3 \log d$ of the lower bound when $q > cd$ for some constant $c > 1$.

Lemma 8. [17] *Let $n > d^{2+\epsilon}$ for some constant $\epsilon > 0$. Any (n, q, d) -PHF is of size at least*

$$\Omega \left(\frac{(q - d + 1)}{q \log(q - d + 2)} \frac{\log n}{g(q, d)} \right).$$

In particular, for $q = d + O(1)$ the bound is

$$\Omega \left(\frac{\log n}{dg(q, d)} \right)$$

and for $q > cd$ for some constant $c > 1$ the bound is

$$\Omega \left(\frac{\log n}{(\log d)g(q, d)} \right).$$

5.3 Dense Perfect Hash

Using Lemma 7 with the same proof as in Theorem 1 we get

Theorem 3. *Let q be a power of prime. If $q > 4(d(d - 1)/2 + 1)/\epsilon$ then there is a $(1 - \epsilon)$ -dense (n, q, d) -perfect hash family of size*

$$O \left(\frac{d^2 \log n}{\epsilon \log(\epsilon q / e(d(d - 1)/2 + 1))} \right)$$

that can be constructed in linear time.

If $(d(d - 1)/2 + 1)/\epsilon + 1 \leq q \leq 4(d(d - 1)/2 + 1)/\epsilon$ then there is a $(1 - \epsilon)$ -dense (n, q, d) -PHF of size

$$O \left(\frac{q^2 d \log n}{\epsilon(q - (d(d - 1)/2 + 1)/\epsilon)^2} \right).$$

that can be constructed in linear time.

The following two folklore results are proved for completeness

Lemma 9. *Let $q \geq d^{1+c}$ for some constant $c > 1$. Any $(1 - \epsilon)$ -dense (n, q, d) -PHF is of size at least*

$$\Omega \left(\frac{d \log n}{\epsilon \log q} \right).$$

Proof. If H is an $(1 - \epsilon)$ -dense (n, q, d) -PHF then any subset of H of size $\epsilon|H| + 1$ is (n, q, d) -PHF. Now the result follows from the lower bound for the size of (n, q, d) -PHF. \square

Lemma 10. *Let $q > d^2/2$. When*

$$\epsilon \leq \frac{d(d-1)}{2q} - \frac{d^2(d-1)^2}{8q^2}$$

then no $(1 - \epsilon)$ -dense (n, q, d) -PHF exists.

Proof. Each hash function $h : [n] \rightarrow [q]$ can be perfect for at most $\binom{q}{d}(n/q)^d$ sets S of size d , [17]. There are exactly $\binom{n}{d}$ sets and therefore the density cannot be greater than

$$1 - \epsilon \leq \frac{\binom{q}{d} \left(\frac{n}{q}\right)^d}{\binom{n}{d}} \xrightarrow{n \rightarrow \infty} \left(1 - \frac{1}{q}\right) \cdots \left(1 - \frac{d-1}{q}\right) \leq e^{-d(d-1)/2q}.$$

Since

$$e^{-d(d-1)/2q} \leq 1 - \frac{d(d-1)}{2q} + \frac{d^2(d-1)^2}{8q^2}.$$

the result follows. \square

For the rest of the paper we will only state the results for the non-dense d -restriction problems. The results for the dense d -restrict problems follows immediately from applying Lemma 7.

5.4 Cover-Free Families

We now prove the following

Theorem 4. *Let $q \geq wr + 2$ be a prime power. Let $S \subseteq \mathbb{F}_q^n$ be a hitting set for \mathcal{H}_{wr} . Given a $(q, (w, r))$ -CFF of size M that can be constructed in linear time one can construct an $(n, (w, r))$ -CFF of size $M \cdot |S|$ that can be constructed in linear time.*

In particular, there is an (w, r) -CFF of size

$$\binom{q}{w} \cdot |S|$$

that can be constructed in linear time in its size.

In particular, for any constant $c > 1$, the following (w, r) -CFF can be constructed in linear time in their sizes

n	w	<i>Linear time.</i> <i>Size=O()</i>	<i>Upper</i> <i>Bound</i>	<i>Lower</i> <i>Bound</i>
<i>all</i>	$O(1)$	$r^{w+1} \log n$	$r^{w+1} \log n$	$\frac{r^{w+1}}{\log r} \log n$
<i>all</i>	$o(r)$	$(ce)^w r^{w+1} \log n$	$\frac{r^{w+1}}{(w/e)^{w-1/2}} \log n$	$\frac{r^{w+1}}{(w/e)^{w+1} \log r} \log n$

Proof. Consider the set of non-zero functions

$$\mathcal{M} = \{\Delta_{\mathbf{i}} \mid \mathbf{i} \in [n]^d, i_1, i_2, \dots, i_d \text{ are distinct}\}$$

where

$$\Delta_{\mathbf{i}}(x_1, \dots, x_n) = \prod_{1 \leq k \leq w \text{ and } w < j \leq d} (x_{i_k} - x_{i_j}).$$

Then S is a hitting set for \mathcal{M} .

Let $\mathcal{F} \subseteq \{0, 1\}^q$ be a $(q, (w, r))$ -CFF of size M . Regard each $f \in \mathcal{F}$ as a function $f : \mathbb{F}_q \rightarrow \{0, 1\}$. It is easy to see that

$$\{(f(b_1), f(b_2), \dots, f(b_n)) \mid b \in S, f \in \mathcal{F}\} \subseteq \{0, 1\}^n$$

is (w, r) -CFF of size $|\mathcal{F}| \cdot |S| = M \cdot |S|$.

Now for every subset $R \subseteq \mathbb{F}_q$ define the function $\chi_R : \mathbb{F}_q \rightarrow \{0, 1\}$ where for $\beta \in \mathbb{F}_q$ we have $\chi_R(\beta) = 1$ if $\beta \in R$ and $\chi_R(\beta) = 0$ otherwise. Then $\{\chi_R \mid R \subseteq \mathbb{F}_q, |R| = w\} \subseteq \{0, 1\}^{\mathbb{F}_q}$ is a $(q, (w, r))$ -CFF of size $\binom{q}{w}$. Therefore

$$C = \{(\chi_R(b_1), \chi_R(b_2), \dots, \chi_R(b_n)) \mid b \in S, R \subseteq \mathbb{F}_q, |R| = w\}$$

is (w, r) -CFF of size

$$|C| \leq \binom{q}{w} |S|.$$

Now for the results in the table consider a constant $c > c' > 1$ and let q be a power of prime such that $q = c'wr + o(wr)$. This is possible by [8]. By Lemma 6 there is a hitting set S for \mathcal{H}_{wr} of size $O(wr \log n)$. This gives a (w, r) -CFF of size

$$O\left(\binom{q}{w} \cdot wr \log n\right) = O\left(\left(\frac{qe}{w}\right)^w wr \log n\right) = O((ce)^w r^{w+1} \log n)$$

that can be constructed in linear time in its size. \square

5.5 Separating Hash Family

Here we prove the following

Theorem 5. *Let $q' > q > D_2$. Let $S \subset \mathbb{F}_{q'}^n$ be a hitting set for \mathcal{H}_{D_2} . Then*

$$M(n, q, \{d_1, d_2, \dots, d_r\}) \leq M(q', q, \{d_1, d_2, \dots, d_r\}) \cdot |S|.$$

In particular, for any constant $c > 1$ and $q > D_2$, the following $(M; n, q, \{d_1, d_2, \dots, d_r\})$ separating hash family can be constructed in linear time

n	q	<i>poly time.</i> <i>Size = $O(\cdot)$</i>	<i>Upper</i> <i>Bound</i>	<i>Lower</i> <i>Bound</i>
<i>all</i>	$q \geq (D_2 + 1)^c$	$D_2^{\frac{\log n}{\log q}}$	$D_1^{\frac{\log n}{\log q}}$	$D_1^{\frac{\log n}{\log q}}$
<i>all</i>	$q \geq c(D_2 + 1)$	$D_2 \log n$	$D_1 \log n$	$D_1^{\frac{\log n}{\log q}}$
<i>all</i>	$q \geq D_2 + 2$	$D_2^3 \log n$	$D_1 \log n$	$D_1^{\frac{\log n}{\log q}}$

and an $(M; n, r, \{d_1, d_2, \dots, d_r\})$ separating hash family of size

$$\binom{cD_2}{d_1 \ d_2 \ \dots \ d_r} D_2 \log n,$$

can be constructed in time linear in the construction size.

Proof. Consider the set of functions

$$\mathcal{F} = \{\Delta_{(C_1, \dots, C_r)}(x_1, \dots, x_n) \mid C_1, \dots, C_r \text{ are pairwise disjoint, } |C_i| = d_i\}$$

in $\mathbb{F}_q[x_1, x_2, \dots, x_n]$ where

$$\Delta_{(C_1, \dots, C_r)} = \prod_{1 \leq k < j \leq r} \prod_{i_1 \in C_k, i_2 \in C_j} (x_{i_1} - x_{i_2}).$$

The proof then proceeds as the proof of Theorem 4 and 1. \square

6 Open Problems

Here we give some open problems

1. Find a polynomial time almost optimal (within $\text{poly}(d)$) construction of (n, q, d) -PHF for $q = o(d^2)$. Using the techniques in [30] it is easy to give an almost optimal construction for (n, q, d) -PHF when $q = d^2/c$ for any constant $c > 1$. Unfortunately the size of the construction is within a factor of $d^{O(c)}$ of the lower bound.

2. In this paper we gave a construction of $(n, (w, r))$ -CFF of size

$$\begin{aligned} & \min((2e)^w r^{w+1}, (2e)^r w^{r+1}) \log n \\ = & \binom{w+r}{r} 2^{\min(w \log w, r \log r)(1+o(1))} \log n \end{aligned} \quad (3)$$

that can be constructed in linear time. Fomin et. al. in [18] gave a construction of size

$$\binom{w+r}{r} 2^{O\left(\frac{r+w}{\log \log(r+w)}\right)} \log n \quad (4)$$

that can be constructed in linear time. The former bound, (3), is better than the latter when $w \geq r \log r \log \log r$ or $r \geq w \log w \log \log w$. We also note that the former bound, (3), is almost optimal, i.e.,

$$\binom{w+r}{r}^{1+o(1)} \log n = N^{1+o(1)} \log n,$$

where $N \log n$ is the optimal size, when $r = w^{\omega(1)}$ or $r = w^{o(1)}$ and the latter bound, (4), is almost optimal when

$$o(w \log \log w \log \log \log w) = r = \omega\left(\frac{w}{\log \log w \log \log \log w}\right).$$

Find a polynomial time almost optimal (within $N^{o(1)}$) construction for (w, r) -CFF when $w = \omega(1)$.

3. A construction is global explicit if it runs in deterministic polynomial time in the size of the construction. A local explicit construction is a construction where one can find any bit in the construction in time poly-log in the size of the construction. The constructions in this paper are linear time global explicit constructions. It is interesting to find local explicit constructions that are almost optimal.

References

- [1] N. Alon. Explicit construction of exponential sized families of k -independent sets, *Discrete Math.* 58 (1986), 191–193.
- [2] N. Alon, D. Moshkovitz, S. Safra. Algorithmic construction of sets for k -restrictions. *ACM Transactions on Algorithms*, 2(2), pp. 153–177. (2006).

- [3] M. Atici, S. S. Magliveras, D. R. Stinson, and W.-D. Wei. Some Recursive Constructions for Perfect Hash Families. *Journal of Combinatorial Designs*. 4(5), pp. 353–363. (1996).
- [4] N. Alon, J. Bruck, J. Naor, M. Naor, R. M. Roth. Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on Information Theory*, 38(2), pp. 509–516. (1992).
- [5] S. R. Blackburn. Perfect Hash Families: Probabilistic Methods and Explicit Constructions. *Journal of Combinatorial Theory, Series A* 92, pp. 54–60 (2000).
- [6] N. H. Bshouty. Testers and their applications. ITCS 2014, pp. 327–352. (2014). Full version: Electronic Colloquium on Computational Complexity (ECCC) 19: 11. (2012).
- [7] S. R. Blackburn, T. Etzion, D. R. Stinson, G. M. Zaverucha. A bound on the size of separating hash families. *Journal of Combinatorial Theory, Series A*, 115(7), pp. 1246–1256. (2008).
- [8] R. C. Baker, G. Harman, J. Pintz. The difference between consecutive primes. II. Proceedings of the London Mathematical Society, 83(3), pp. 532–562. (2001).
- [9] S.G. Barwick, ,Wen-Ai Jackson. Geometric constructions of optimal linear perfect hash families. *Finite Fields and Their Applications*. 14(1), pp 1–13. (2008).
- [10] S. G. Barwick, Wen-Ai Jackson, C. T. Quinn. Optimal Linear Perfect Hash Families with Small Parameters. *Journal of Combinatorial Designs*, 12(5), pp. 311–324. (2004).
- [11] M. Bazrafshan, T. van Trung. Bounds for separating hash families. *Journal of Combinatorial Theory, Series A*, 118(3), pp. 1129–1135. (2011).
- [12] S. R. Blackburn, P. R. Wild. Optimal linear perfect hash families. *Journal of Combinatorial Theory, Series A*, 83(2), pp. 233–250. (1998).
- [13] D. Z. Du, F. K. Hwang. Combinatorial group testing and its applications. Volume 12 of Series on Applied Mathematics. World Scientific, New York, second edition, (2000).

- [14] A. G. Dýachkov and V. V. Rykov. Bounds on the length of disjunctive codes. *Problemy Peredachi Inf*, 18(3), pp. 7–13. (1982).
- [15] A. G. Dýachkov, V. V. Rykov, A. M. Rashad. Superimposed distance codes. *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, 18(4), pp. 237–250. (1989).
- [16] Z. Füredi. On r -cover-free families. *Journal of Combinatorial Theory, Series A*, 73(1), pp. 172–173. (1996).
- [17] M. L. Fredman, J. Komlós. On the size of separating systems and families of perfect hash function, *SIAM J. Algebraic and Discrete Methods*, 5(1), pp. 61–68. (1984).
- [18] F. V. Fomin, D. Lokshtanov, S. Saurabh. Efficient Computation of Representative Sets with Applications in Parameterized and Exact Algorithms. *SODA 2014*, pp. 142–151. (2014).
- [19] P. Indyk, H. Q. Ngo, A. Rudra. Efficiently decodable non-adaptive group testing. In the 21st Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 10), pp. 1126–1142. (2010).
- [20] J. Körner. Fredman-Komlós bounds and information theory, *SIAM J. Algebraic and Discrete Methods*, 7(4), pp. 560–570. (1986).
- [21] J. Körner, K. Marton. New bounds for perfect hashing via information theory. *Europ. J. of Combinatorics*, 9(6), pp. 523–530. (1988).
- [22] W. H. Kautz, R. C. Singleton, Nonrandom binary superimposed codes, *IEEE Trans. Inform. Theory*, 10(4), pp. 363–377. (1964).
- [23] L. Liu, H. Shen. Explicit constructions of separating hash families from algebraic curves over finite fields. *Designs, Codes and Cryptography*, 41(2), pp. 221–233. (2006).
- [24] S. Martirosyan. Perfect Hash Families, Identifiable Parent Property Codes and Covering Arrays. Dissertation zur Erlangung des Grades eines Doktors der Naturwissenschaften. (2003).
- [25] K. Mehlhorn, On the program size of perfect and universal hash functions. *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS82)*, (1982), pp. 170–175.

- [26] S. Martirosyan, T. van Trung Explicit constructions for perfect hash families. *Designs, Codes and Cryptography* January 2008, 46(1), pp. 97–112.
- [27] A. Nilli. Perfect hashing and probability. *Combinatorics, Probability and Computing*, 3(3), pp. 407–409. (1994).
- [28] H. Q. Ngo, D. Z. Du. A survey on combinatorial group testing algorithms with applications to DNA library screening. *Theoretical Computer Science*, 55, pp. 171-182. (2000).
- [29] J. Naor, M. Naor. Small-bias probability spaces: efficient constructions and applications. *SIAM J. Comput.*, 22(4), pp. 838–856. (1993).
- [30] M. Naor, L. J. Schulman, A. Srinivasan. Splitters and Near-optimal Derandomization. *FOCS 95*, pp. 182–191, (1995).
- [31] E. Porat, A. Rothschild. Explicit Nonadaptive Combinatorial Group Testing Schemes. *IEEE Transactions on Information Theory* 57(12), pp. 7982–7989 (2011).
- [32] D. R. Stinson, R. Wei, L. Zhu. New constructions for perfect hash families and related structures using combinatorial designs and codes, *J. Combin. Designs.*, 8(3), pp. 189-200. (2000).
- [33] D.R. Stinson, R. Wei, K. Chen. On generalised separating hash families. *Journal of Combinatorial Theory, Series A*, 115(1), pp. 105–120. (2008).
- [34] D. R. Stinson, R. Wei, L. Zhu. Some new bounds for cover-free families, *Journal of Combinatorial Theory, Series A*, 90(1), pp. 224-234. (2000).
- [35] D.R. Stinson, T. van Trung, R. Wei. Secure frameproof codes, key distribution patterns, group testing algorithms and related structures, *J. Stat. Planning and Inference*, 86(2), pp. 595-617. (2000).
- [36] H. Wang and C. P. Xing. Explicit Constructions of perfect hash families from algebraic curves over finite fields. *J. of Combinatorial Theory, Series A*, 93(1), pp. 112–124. (2001).